The Honourable Society of Gray's Inn

Data Protection Policy

1. Introduction

The Honourable Society of Gray's Inn ("the Society") needs to collect and use certain types of information about the Individuals who come into contact with the Society in order to carry on our work. This personal information must be collected and dealt with appropriately and there are safeguards to ensure this under the Data Protection Act 1998.

2. Data Controller

The Society is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

The Society may share data with other agencies, such as the Bar Standards Board or the Council of the Inns of Court, who have a responsibility for the regulation of barristers.

The Individual will be made aware how and with whom their information will be shared. There are circumstances where the law allows the Society to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of the Individual or other person

c) The Individual has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the Individual User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals to provide consent signatures.

4. Data Protection Principles

The Society intends to ensure that personal information is treated lawfully and correctly. To this end, the Society will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

c) Shall be adequate, relevant and not excessive in relation to those purpose(s)

d) Shall be accurate and, where necessary, kept up to date,

e) Shall not be kept for longer than is necessary

f) Shall be processed in accordance with the rights of data subjects under the Act,

g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or damage to personal information,

h) Shall not be transferred to a country or territory outside the European Economic Area.

The Society will**:**

- Observe conditions regarding the fair collection and use of information
- Specify the purposes for which information is used
- Collect and process appropriate information only to the extent that it is needed to fulfill its needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate security measures to safeguard personal information

- Ensure that personal information is not transferred outside the European Economic Area without suitable safeguards

- Treat people fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

- Set out clear procedures for responding to requests for information

- Maintain documentation, including a data asset register, detailing the controls, systems and processes which will ensure that the above aims are met.

5. Data collection

Data will be collected with the informed consent of the individual. Informed consent is when:

- An Individual clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- And then gives their consent.

The Society will ensure that data is collected as laid down by this policy.

When collecting data, the Society will ensure that the Individual:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

6. Data Storage

Information and records containing personal data will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is the Society's responsibility to ensure all personal data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

7. Data access and accuracy

All Individuals have the right to access the information the Society holds about them. The Society will respond to Subject Access Requests within the timetable stipulated, and upon payment of any fee permitted, by legislation.

In addition**,** the Society will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection. Contact details for the Data Protection Officer will be shown on the Society's web-site.

- All those processing personal information understand that they are responsible for following good data protection practice

- All those processing personal information are appropriately trained and supervised

- All those handling personal information know how to seek instruction or guidance if required

- It deals promptly and courteously with any enquiries about handling personal information

- It describes clearly how it handles personal information

- It will regularly review the ways it holds, manages and uses personal information

- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Society's Data Protection Officer:

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information the Society will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person (s) responsible for ensuring that the Society follows its data protection policy and complies with the Data Protection Act 1998.

Individual – The person whose personal information is being held or processed by the Society for example: client, employee, student, member or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of the Society, as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings
- Disciplinary proceedings